Aiello 1999-0053

REMARKS

Claims 1-4, 9, 11-15, 20, 22-26, 31 and 33 were rejected under 35 USC 102 as being anticipated by US Patent No. 5,153,919 issued to Reeds III et al. Applicants respectfully traverse.

Claim 1 specifies a provisioning server. The Examiner asserts that Reeds III et al teach "receiving information authenticating a provisioning server (base station, Reeds, col. 3, line 21-23)." This establishes that, according to the Examiner, the provisioning server correspondence to the base station, i.e., the visited CGSA in FIG. 3.

The cited passage states (extended to include the beginning and the end of the sentence):

> Thereafter the mobile unit communicates with the base station with the assistance of authentication processes that are carried out between the mobile unit and the base station, using the shared secret data field.

Alas, this sentence lacks meaning without knowing the context of the "thereafter." What the preceding two sentences say is:

> When a mobile unit enters the cell of a base station, it identifies itself to the base station, and supplies to the base station a hashed authentication string. The base station consults with the provider, and if it is determined that the mobile unit is a bona fide unit, the provider supplies the base station with the shared secret data field.

Hence, it should be understood that there is an authentication process by which the mobile unit gets authenticated to the base station, and thereafter the mobile unit communicates with the base station "with the assistance of authentication processes ... using the shared secret data field. Respectfully, that is NOT a teaching of a step of receiving information that authenticates a provisioning server (i.e., the base station). It is respectfully that in the remainder of the reference there is also no teaching or suggestion for authenticating the base station. Therefore the claim 1 is not anticipated by Reeds III et al.

The Examiner also points to col. 5, lines 60-61 as teaching the authentication string of claim 1. Applicants respectfully disagree. The cited text discusses inputs to the Jumble process, which text effectively states that any string can be thought of as an authentication string, and that there is no real difference between data and a key (at least when in comes to a Jumble process). The Examiner further asserts that the authentication

string is taught, and although the Examiner does not state what that string is, it is true that an RANDSSD string is sent by the home CGSA to the user. However, although the RANDSSD can be viewed as an authentication string, or as a key, it is NOT POSSIBLE to assert that the RANDSSD sting corresponds to a cryptographic key that had been encrypted, as claim 1 specifies.

Therefore, it is respectfully submitted that the claim 1 is not anticipated by the Reeds III et al reference.

As for new independent claim 34, it specifies a step of sending a request to a provisioning server. Reeds III et al do not describe such a step. The claim also specifies receiving a key of the provisioning server AND information that authenticates the provisioning server. No such authenticating information is received in the arrangement described in Reeds III et al. The claim further specifies a step of generating various random keys. No such step is described or suggested in Reeds III et al. The claim still further specifies a step of sending keys to the provisioning server. No such step is described or suggested in Reeds III et al. Since there is no step of sending keys, it is not surprising that there is no step of the provisioning server sending an acknowledgement. In short, none of the method steps of claim 34 are found in Reeds III et al and, therefore, it is respectfully submitted that claim 34 is neither anticipated nor made obvious by the Reeds III et al reference.

Since claim 34 is neither anticipated nor made obvious by the Reeds III et al reference, it follows that claims 2-11 and 35-39, which depend on claim 34 are also neither anticipated nor made obvious by the reference.

As for independent apparatus claim 12, it is respectfully submitted that, for the reasons expressed in connection with claim 1 and claim 34, claim 12 and the claims that depend on claim 12 are neither anticipated nor made obvious by Reeds III et al.

It is respectfully submitted that the various amendments that were made to the claims were made for reasons other than for the purpose of distinguishing such claim from known prior art -- as is evidenced by the fact that claim 1 was NOT amended, and per force of applicants' arguments relative to claim 1. These amendments are not being made with any intent to change in any way the literal scope of such claims or the range of equivalents for such claims. They are being made, rather, simply to present language that

Aiello 1999-0053

is better in conformance with the form requirements of Title 35 of the United States Code or is simply clearer and easier to understand than the originally presented language.

In light of the above amendments and remarks, applicants respectfully submit that all of the Examiner's rejections have been overcome. Reconsideration and allowance of all outstanding claims are respectfully solicited.

Respectfully,
William A. Aiello
Charles R. Kalmanek
Steven Michael Bellovin
William Todd Marshall
Aviel D. Rubin

Dated: 4/30/04

By 

Henry T. Brendzel
Reg. No. 26,844
Phone (973) 467-2025
Fax (973) 467-6589
email brendzel@comcast.net